======= WPI =======

TI - Data transmission method for broadcasting system - in which scramble key currently used by scrambler for carrying out data scrambling is set as first key and recognition code indicating second key which is used after first key is transmitted

AB - J08331119 The method involves generating predetermined timing for altering a set of multiple scramble keys in an orderly manner using a generation unit. A scrambler (14) carries out scrambling of a data using the scramble key set by the generation unit.
- The key currently used by the scrambler for carrying data scrambling is set as the first key and the key to be used next is set as second key. A recognition code indicating the second scramble key is transmitted by a transmission part.
- ADVANTAGE - Enables starting of descramble at suitable timing by transmitting scramble key to be used next. Enables orderly updation of scramble keys.
- (Dwg.5/6)

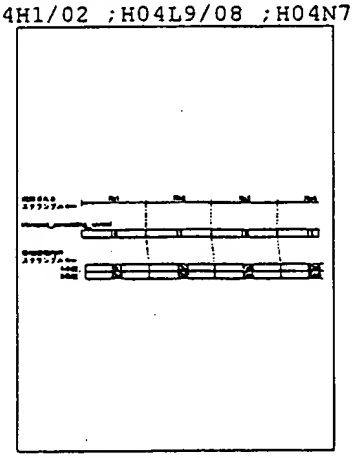
PN - JP8331119 A 19961213 DW199709,H04L9/16 008pp
PR - JP19950133121 19950531
PA - (SONY) SONY CORP
MC - W01-A05A W02-D01 W02-F05A1 W02-F10N1
DC - P85 W01 W02
IC - G09C1/00 ;H04H1/02 ;H04L9/08 ;H04L9/16 ;H04N7/169
AN - 1997-093584 [09]

======= PAJ =======

TI - DEVICE AND METHOD FOR DATA TRANSMISSION AND DEVICE AND METHOD FOR DATA RECEPTION

AB - PURPOSE: To start descrambling at an arbitrary timing even when a scramble key is updated sequentially.
- CONSTITUTION: The scramble key is changed to Ks1 , Ks2 , Ks3 , Ks4 ,... at a prescribed timing sequentially. Also, two scramble keys of systems A and B are transmitted as program information, and one of them is set as the scramble key in current use, and the other as the one to be used next. Moreover, an identification code representing the scarmble key in current use is transmitted as transport-scrambling-control.

PN - JP8331119 A 19961213
PD - 1996-12-13
ABD - 19970430
ABV - 199704
AP - JP19950133121 19950531
PA - SONY CORP
IN - YAMASHITA MASAMI;YOSHIDA HIROYUKI
I - H04L9/16 ;G09C1/00 ;H04H1/02 ;H04L9/08 ;H04N7/169



<First Page Image>

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－331119

(43)公開日　平成８年(1996)12月13日

(51)Int.Cl.⁶		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	9/16		8842－5Ｊ	Ｈ０４Ｌ	9/00	６４３
Ｇ０９Ｃ	1/00	６３０	7259－5Ｊ	Ｇ０９Ｃ	1/00	６３０Ｂ
Ｈ０４Ｈ	1/02			Ｈ０４Ｈ	1/02	Ｅ
Ｈ０４Ｌ	9/08		8842－5Ｊ	Ｈ０４Ｌ	9/00	６０１Ｂ
Ｈ０４Ｎ	7/169			Ｈ０４Ｎ	7/167	Ａ

審査請求　未請求　請求項の数７　ＯＬ　（全８頁）

(21)出願番号　特願平7－133121

(22)出願日　平成７年(1995)５月31日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　山下　雅美
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　吉田　洋之
東京都品川区北品川６丁目７番35号　ソニー株式会社内

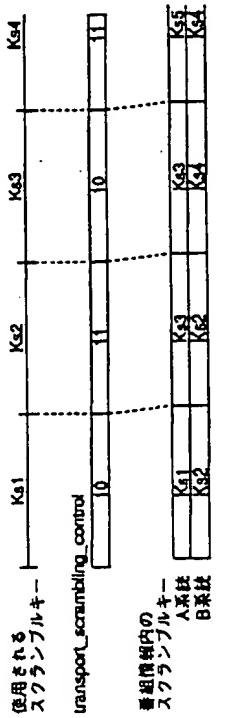
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　データ伝送装置および方法並びにデータ受信装置および方法

(57)【要約】

【目的】　スクランブルキーを順次更新する場合においても、任意のタイミングからデスクランブルを開始することができるようにする。

【構成】　スクランブルキーをＫｓ₁，Ｋｓ₂，Ｋｓ₃，Ｋｓ₄，…と、所定のタイミングで順次変更する。また、番組情報としてＡ系統とＢ系統の２つのスクランブルキーを伝送するようにし、その一方は現在使用中のスクランブルキーとし、他方はその次に使用されるスクランブルキーとする。さらに、ｔｒａｎｓｐｏｒｔ＿ｓｃｒａｍｂｌｉｎｇ＿ｃｏｎｔｒｏｌとして、現在使用しているスクランブルキーを表す識別コードを伝送する。



1

【特許請求の範囲】

【請求項1】　伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生する発生手段と、
前記発生手段が発生したキーを用いて前記データをスクランブルするスクランブル手段と、
前記スクランブル手段が前記データをスクランブルするのにそのとき用いられている第1のキーと、その次に用いられる第2のキーを伝送する伝送手段とを備えることを特徴とするデータ伝送装置.

【請求項2】　前記伝送手段は、前記第1のキーと前記第2のキーを、同時に伝送することを特徴とする請求項1に記載のデータ伝送装置.

【請求項3】　前記伝送手段は、伝送するキーのうち、現在用いられている前記第1のキーがいずれであるのかを表す識別信号をさらに伝送することを特徴とする請求項2に記載のデータ伝送装置.

【請求項4】　伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生し、
発生された前記キーを用いて前記データをスクランブルし、
前記データをスクランブルするのにそのとき用いられている第1のキーと、その次に用いられる第2のキーを伝送することを特徴とするデータ伝送方法.

【請求項5】　伝送されてきたデータをスクランブルするのにそのとき用いられている第1のキーと、その次に用いられる第2のキーを抽出する抽出手段と、
前記抽出手段により抽出された前記キーから、前記第1のキーを選択する選択手段と、
前記選択手段により選択された前記第1のキーを用いて、前記データをデスクランブルするデスクランブル手段とを備えることを特徴とするデータ受信装置.

【請求項6】　伝送されてきた複数の前記キーのいずれが前記第1のキーであるのかを表す識別信号を検出し、検出した前記識別信号に対応して前記選択手段を制御する検出手段をさらに備えることを特徴とする請求項5に記載のデータ受信装置.

【請求項7】　伝送されてきたデータをスクランブルするのにそのとき用いられている第1のキーと、その次に用いられる第2のキーを抽出し、
抽出された前記キーから、前記第1のキーを選択し、
選択された前記第1のキーを用いて、前記データをデスクランブルすることを特徴とするデータ受信方法.

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、データ伝送装置および方法並びにデータ受信装置および方法に関し、特にスクランブルキーが更新された場合においても、スクランブルされているデータを迅速にデスクランブルすることができるようにしたデータ伝送装置および方法並びにデータ受信装置および方法に関する.

2

【0002】

【従来の技術】有料放送においては、データをスクランブルして放送することが多い.この有料放送の視聴を希望する者は、放送局と契約をし、デコーダを取得する.そして、このデコーダにより、スクランブルされているデータをデスクランブルして、正常な画像、音声、データなどを得るようにする.

【0003】このようなスクランブル放送においては、契約をしていない者がスクランブル放送を実質的に受信することができないようにする必要がある.すなわち、スクランブルされているデータが容易にデスクランブルされないように、その秘密性を高める必要がある.そのため、スクランブルキーを所定の期間毎に、新たなスクランブルキーに更新し、スクランブルキーを使い捨てにする方法が提案されている.

【0004】図6は、このようなスクランブルキーを更新する従来の例を表している.この例においては、時刻t_1からスクランブルキーK1が用いられ、時刻t_2から、このスクランブルキーK1がスクランブルキーK2に更新される.そして、時刻t_3においては、スクランブルキーK3に、時刻t_4においては、スクランブルキーK4に、それぞれ更新される.すなわち、これらのスクランブルキーを用いてデータをスクランブルして、スクランブルデータが放送される.

【0005】デコーダ側においては、このスクランブルキーを予め取得しておかないと、受信したスクランブルデータをデスクランブルすることができない.そこで、送信側においては、スクランブルキーを更新する前に、次に使用するスクランブルキーを伝送するようにしている.例えば、時刻t_2において、スクランブルキーがK1からK2に変更される場合、時刻t_2までの期間、次に使用されるスクランブルキーとしてK2を伝送する.デコーダ側においては、このK2をメモリに予め記憶しておき、時刻t_2において、スクランブルキーが更新されたとき、更新された（メモリに記憶されている）スクランブルキーK2を用いてデスクランブルを行うようにする.

【0006】また、このとき、送信側は、時刻t_2において、次に使用するスクランブルキーとして、K2に代えてK3を伝送する.デコーダ側においては、スクランブルキーK2を用いて、デスクランブルを行っている間に、次に更新されるスクランブルキーとして、K3をメモリに記憶する.

【0007】以上のようにして、スクランブルキーが順次更新された場合においても、スクランブルされているデータを正しくデスクランブルことが可能となる.

【0008】

【発明が解決しようとする課題】しかしながら、従来の装置においては、次に用いられるスクランブルキーだけ

を伝送するようにしているため、スクランブル放送の受信開始のタイミングによっては、最悪の場合、次にスクランブルキーが更新されるまで、スクランブル放送をデスクランブルすることができない場合があった。

【0009】例えば、図6に示すように、時刻t_2において、スクランブルキーがＫ１からＫ２に変更されたような場合、時刻t_2の直後の時刻t_{21}において、スクランブル放送の受信を開始すると、そのとき、放送局側から送られてくるスクランブルキーは、次に更新されるスクランブルキーＫ３であるため、現在のスクランブルに用いられているスクランブルキーＫ２を得ることができない。その結果、受信を開始した時刻t_{21}から、次にスクランブルキーがＫ２からＫ３に更新される時刻t_3までの期間T_2の間、実質的にスクランブルデータをデスクランブルすることができないことになる。

【0010】本発明はこのような状況に鑑みてなされたものであり、スクランブルキーが適宜更新される場合にあっても、迅速にデスクランブルを開始することができるようにするものである。

【0011】

【課題を解決するための手段】請求項１に記載のデータ伝送装置は、伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生する発生手段と、発生手段が発生したキーを用いてデータをスクランブルするスクランブル手段と、スクランブル手段がデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを伝送する伝送手段とを備えることを特徴とする。

【0012】請求項４に記載のデータ伝送方法は、伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生し、発生されたキーを用いてデータをスクランブルし、データをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを伝送することを特徴とする。

【0013】請求項５に記載のデータ受信装置は、伝送されてきたデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを抽出する抽出手段と、抽出手段により抽出されたキーから、第１のキーを選択する選択手段と、選択手段により選択された第１のキーを用いて、データをデスクランブルするデスクランブル手段とを備えることを特徴とする。

【0014】請求項７に記載のデータ受信方法は、伝送されてきたデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを抽出し、抽出されたキーから、第１のキーを選択し、選択された第１のキーを用いて、データをデスクランブルすることを特徴とする。

【0015】

【作用】請求項１に記載のデータ伝送装置においては、

発生手段が、伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生し、スクランブル手段が、発生手段が発生したキーを用いてデータをスクランブルし、伝送手段が、スクランブル手段がデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを伝送する。

【0016】請求項４に記載のデータ伝送方法においては、データをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーが伝送される。

【0017】請求項５に記載のデータ受信装置においては、抽出手段が、伝送されてきたデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを抽出し、選択手段が、抽出手段により抽出されたキーから、第１のキーを選択し、デスクランブル手段が、選択手段により選択された第１のキーを用いて、データをデスクランブルする。

【0018】請求項７に記載のデータ受信方法においては、伝送されてきたデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーが抽出され、抽出された第１のキーを用いて、データがデスクランブルされる。

【0019】

【実施例】以下に、本発明の実施例を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施例との対応関係を明らかにするために、各手段の後の括弧内に対応する実施例（ただし、一例）を付加して、本発明の特徴を記述すると、次のようになる。

【0020】すなわち、請求項１に記載のデータ伝送装置は、伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生する発生手段（例えば図１のスクランブル制御システム１６、関連情報送出装置１７）と、発生手段が発生したキーを用いてデータをスクランブルするスクランブル手段（例えば図１のスクランブラ１４）と、スクランブル手段がデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを伝送する伝送手段（例えば図１の多重化器１３）とを備えることを特徴とする。

【0021】請求項５に記載のデータ受信装置は、伝送されてきたデータをスクランブルするのにそのとき用いられている第１のキーと、その次に用いられる第２のキーを抽出する抽出手段（例えば図２の復号器４２，４３）と、抽出手段により抽出されたキーから、第１のキーを選択する選択手段（例えば図２の選択回路３３）と、選択手段により選択された第１のキーを用いて、データをデスクランブルするデスクランブル手段（図２のデスクランブラ３２）とを備えることを特徴とする。

【0022】請求項６に記載のデータ受信装置は、伝送

されてきた複数のキーのいずれが第１のキーであるのかを表す識別信号を検出し、検出した識別信号に対応して選択手段を制御する検出手段（例えば図２のフラグ検出回路４５）をさらに備えることを特徴とする。

【００２３】ただし、もちろん、この記載は、各手段を上記したものに限定することを意味するものではない。

【００２４】図１は、本発明が適用される放送システムの構成例を表している。この実施例においては、送信装置１が伝送路３を介してスクランブルデータを、各家庭の受信端末２に伝送（放送）し、受信端末２がこれを受信するようになされている。そして、受信端末２は、伝送路３を介して受信した放送に関する視聴情報を、必要に応じて、電話回線４を介して、送信装置１に送信するようになされている。

【００２５】送信装置１の番組制御システム１１は、放送すべき映像信号や音声信号を含む信号をエンコーダ１２に供給するようになされている。エンコーダ１２は、入力された映像信号と音声信号をA／D変換し、得られたデータをMPEG2 Video（ISO（International Organization for Standardization）／IEC（International Electoro-technical Comission）13818－2），MPEG2 Audio（ISO／IEC13818－3）で規定される方式に従ってエンコードし、エンコードしたデータを多重化器１３に供給するようになされている。また、番組制御システム１１は、エンコーダ１２に出力した映像信号と音声信号に対応する番組の番組番号を関連情報送出装置１７に出力している。

【００２６】視聴情報収集処理システム１５は、電話回線４を介して、各受信端末２から伝送されてきた視聴情報や、視聴者からの契約要求を処理して、契約情報としてスクランブル制御システム１６に出力する。スクランブル制御システム１６は、内蔵するメモリ１６Aに、各受信端末２に対応するマスターキーKmを記憶している。そして、このマスターキーKmを用いて暗号化したワークキーKwを発生し、関連情報送出装置１７に出力している。また、スクランブル制御システム１６は、加入者毎の契約情報とワークキーKwを含む個別情報を、対応する受信端末のデコーダＩＤを付加して多重化器１３に出力している。

【００２７】関連情報送出装置１７は、スクランブル制御システム１６より供給されたワークキーKwを用いて暗号化したスクランブルキーKsiを発生し、スクランブラ１４に出力している。また、関連情報送出装置１７は、番組番号、スクランブルキーKsi、およびその他の番組に関する情報を含む番組情報と、受信端末２のデコーダ２１のデスクランブル機能を強制的にオンまたはオフさせる指令である制御情報とからなる共通情報を多重化器１３に出力している。

【００２８】スクランブラ１４に供給されるスクランブルキーKsiは、所定のタイミングで新たなキーに更新される。また、番組情報には、そのとき使用されているスクランブルキーKsiと、次に使用されるスクランブルキーKs（i＋1）が含められる。

【００２９】多重化器１３は、ワークキーKwを含む個別情報、関連情報送出装置１７が出力するスクランブルキーKsiを含む番組情報を含む共通情報、およびエンコーダ１２より供給される音声データおよび映像データを、それぞれMPEG2 Systems（ISO／IEC13818－1）の規定に従ってパケット化して多重化し、スクランブラ１４に出力する。スクランブラ１４は、関連情報送出装置１７より供給されるスクランブルキーKsiを用い、多重化器１３より供給される映像データと音声データをスクランブルする。ただし、共通情報と個別情報は、スクランブルしない。スクランブラ１４の出力は、伝送路３（電波あるいはケーブル）を介して受信端末２に伝送される。

【００３０】なお、送信装置１においては、実際には、スクランブラ１４の後段に、誤り訂正符号化回路、変調回路などが必要となるが、ここでは省略する。

【００３１】受信端末２においては、伝送路３を介して伝送されてきたデータがデコーダ２１に供給され、デコードされるようになされている。デコーダ２１は、伝送路３を介して入力されたデータのうち、共通情報と個別情報をセキュリティモジュール２２に供給する。ＩＣカードなどで構成されるセキュリティモジュール２２は、共通情報および個別情報に対応して、視聴制御情報を発生し、デコーダ２１に出力している。

【００３２】図２は、デコーダ２１とセキュリティモジュール２２の一部の構成例を表している。伝送路３を介して入力されたデータは、デコーダ２１の分離回路３１に入力されるようになされている。分離回路３１は、入力されたデータをパケット毎に分離し、映像データと音声データをデスクランブラ３２に供給し、その他のデータをセキュリティモジュール２２の分離回路４７に供給する。

【００３３】分離回路４７は、入力されたデータからトランスポートパケットのパケットヘッダを分離し、フラグ検出回路４５に供給している。フラグ検出回路４５は、トランスポートパケットのパケットヘッダに含まれるtransport_scrambling_control（識別信号）を検出し、その検出結果をデコーダ２１の選択回路３３に出力するようになされている。

【００３４】さらにまた、分離回路４７は、メモリ４１に記憶されているデコーダＩＤに対応するＩＤを有する個別情報を分離し、復号器４２に出力するとともに、番組情報を分離し、復号器４３に出力している。

【００３５】復号器４２にはまた、メモリ４４に記憶されているマスターキーKmが供給されており、復号器４

2は、このマスターキーKmを利用して個別情報に含まれるワークキーKwを復号化し、復号器43に出力している。復号器43は、復号器42より供給されるワークキーKwを用いて、番組情報に含まれるスクランブルキーKsiを復号化し、選択回路33に出力している。

【0036】このスクランブルキーKsiとしては、現在伝送されているスクランブルデータのスクランブルに用いられているスクランブルキーKsiと、次の更新時に用いられるスクランブルキーKs（i+1）の2種類が存在する。選択回路33は、この2種類のスクランブルキーのうち、現在用いられているスクランブルキーをフラグ検出回路45の出力に対応して選択し、選択したスクランブルキーKsiをデスクランブラ32に供給している。デスクランブラ32は、選択回路33より供給されたスクランブルキーKsiを用いて、分離回路31より入力された映像データと音声データとをデスクランブルし、出力するようになされている。

【0037】次に、その動作について説明する。エンコーダ12は、番組制御システム11より供給される映像信号と音声信号とをデジタル化し、MPEG方式でエンコード（圧縮）する。そして、エンコードした音声データと映像データは、多重化器13に供給される。多重化器13は、入力された映像データと音声データを、図3に示すトランスポートパケットのフォーマットに従って、パケット化する。

【0038】すなわち、1トランスポートパケットの長さは188バイトとされ、その先頭の4バイトはヘッダ、残りの184バイトはデータ部とされ、そこに音声データや映像データなどの実データが配置されるようになされている。

【0039】ヘッダには、その先頭に8ビットの同期バイトが配置され、続く3ビットには、transport_error_indicator，payload_unit_start_indicatorおよびtransport_priorityが1ビットずつ配置されている。さらに、それに続く13ビットには、音声データ、映像データ、共通情報、個別情報などのデータを識別するパケットIDが配置されている。

【0040】次の2ビットは、transport_scrambling_controlとされ、その次の2ビットは、adaption_field_controlとされ、最後の4ビットは、continuity_counterとされている。

【0041】映像データと音声データは、このトランスポートパケットのデータ部に配置され、そのパケットIDには、音声データまたは映像データであることを表すパケットIDが配置される。

【0042】スクランブラ14は、多重化器13より供給された音声データおよび映像データのトランスポートパケットを、関連情報送出装置17より供給されるスクランブルキーKsiを用いてスクランブルし、伝送路3を介して伝送する。

【0043】このスクランブルキーKsiは、次のように生成される。すなわち、スクランブル制御システム16は、メモリ16Aに記憶されているマスターキーKmを用いて暗号化したワークキーKwを発生する。関連情報送出装置17は、このワークキーKwを用いて暗号化したスクランブルキーKsiを発生し、スクランブラ14に供給する。

【0044】このスクランブルキーKsiとしては、本出願人が先に提案した、例えば特願平6－328027、特願平6－328559、特願平7－802などに記載のものを用いることができる。

【0045】関連情報送出装置17は、図4に示すように、スクランブルキーKsiを所定の時間毎に、Ks_1，Ks_2，Ks_3，Ks_4，…のように、順次更新（変更）する。

【0046】また、関連情報送出装置17は、このスクランブルキーの更新に対応して、番組情報の一部として、A系統とB系統の2つのスクランブルキーを伝送させる。

【0047】例えば、図4に示すように、スクランブラ14にスクランブルキーKs_1を供給しているとき、番組情報には、A系統のスクランブルキーとして、Ks_1を配置し、B系統のスクランブルキーとしては、次に使用するスクランブルキーKs_2を配置する。

【0048】そして、スクランブラ14に供給するスクランブルキーをKs_1からKs_2に変更したときは、B系統のスクランブルキーとして、そのままKs_2を伝送し、A系統のスクランブルキーとしては、次に使用されるスクランブルキーKs_3を伝送する。

【0049】そして、スクランブラ14に供給するスクランブルキーを、Ks_2からKs_3に変更した場合においては、A系統のスクランブルキーは、Ks_3のままとし、B系統のスクランブルキーは、次に使用するスクランブルキーKs_4に変更する。

【0050】このように、番組情報の一部として、現在使用中のスクランブルキーと、次に使用されるスクランブルキーとを、同時に伝送するようにする。

【0051】また、関連情報送出装置17は、多重化器13を制御し、図3に示すトランスポートパケットのヘッダのtransport_scrambling_controlに、A系統とB系統のスクランブルキーのうち、現在使用されているスクランブルキーが、いずれの系統のスクランブルキーであるのかを表す識別データを伝送させる。

【0052】例えば、図5に示すように、A系統のスクランブルキーを現在使用している場合においては、識別データとして10を伝送し、B系統のスクランブルキーを使用している場合においては、識別データとして11

を伝送させる。

【0053】図4に示すように、transport_scrambling_controlにおける識別データの更新は、スクランブルキーの更新に同期して行われる。

【0054】これに対して、番組情報内におけるA系統とB系統のスクランブルキーの更新は、使用されるスクランブルキーの更新後であって、比較的近い時刻であればよく、使用されるスクランブルキーの更新時期と必ずしも正確に同期している必要はない。換言すれば、使用されるスクランブルキーの更新時期と番組情報内のスクランブルキーの更新時期とは、密の結合関係にある必要はなく、粗の結合関係にあればよい。

【0055】多重化器13は、音声データと映像データとを上述したようにパケット化して伝送するのと同様に、個別情報と共通情報もパケット化して伝送する。ただし、この共通情報と個別情報は、スクランブラ14によりスクランブルされずに伝送される。

【0056】一方、伝送路3を介して送信装置1より伝送されてきたデータは、デコーダ21の分離回路31に入力される。分離回路31は、入力されたパケットのパケットIDから、そのトランスポートパケットのデータ部のデータの種類を判別し、音声データと映像データは、デスクランブラ32に供給し、その他のデータを分離回路47に供給する。

【0057】分離回路47は、A系統とB系統のスクランブルキーKsiを含む番組情報のパケットを分離し、復号器43に出力する。

【0058】さらに、分離回路47は、メモリ41に記憶されているデコーダIDに対応するパケットIDの個別情報が入力された場合においてはこれを分離し、ワークキーKwを含むその個別情報を復号器42に出力する。

【0059】復号器42は、メモリ44に予め記憶されているマスターキーKmを利用して分離回路31より供給された個別情報に含まれるワークキーKwを復号化し、復号器43に出力する。

【0060】復号器43は、復号器42より供給されたワークキーKwを利用して、分離回路31より供給された番組情報に含まれるA系統とB系統のスクランブルキーKsiを復号化し、選択回路33に出力する。

【0061】分離回路47はまた、入力されたトランスポートパケットのパケットヘッダを分離し、フラグ検出回路45に出力する。フラグ検出回路45は、入力されたパケットヘッダのうち、現在使用されているスクランブルキーを表す識別コードが含まれているtransport_scrambling_controlを検出し、その検出結果を選択回路33に出力する。

【0062】選択回路33は、フラグ検出回路45からの検出結果に対応して復号器43より供給されるA系統とB系統の2つのスクランブルキーKsiのうち、現在使用されているスクランブルキーを選択し、デスクランブラ32に供給する。すなわち、transport_scrambling_controlが10であるときA系統のスクランブルキーを選択し、11であるときB系統のスクランブルキーを選択する。デスクランブラ32は、選択回路33より供給された現在使用されているスクランブルキーKsiを用いて、分離回路31より供給されたスクランブルされている音声データおよび映像データをデスクランブルし、出力する。

【0063】図4に示すように、例えば現在使用されているスクランブルキーがKs_2である場合、このスクランブルキーKs_2は、その直前のスクランブルキーKs_1が使用されている状態の時からB系統のスクランブルキーとして伝送されてきており、また、スクランブルキーが、Ks_2からKs_3に変更された直後まで、B系統のスクランブルキーとして伝送されてくる。従って、このスクランブルキーKs_2は、データをスクランブルするのに必要なタイミングにおいて、常に得ることができる。その結果、どのタイミングにおいて受信を開始したとしても、現在使用中のスクランブルキーを得ることができ、受信を開始したとき、直ちにデスクランブルを実行することができる。

【0064】以上、本発明を、映像データと音声データとをデジタル化し、スクランブルして伝送する場合を例として説明したが、本発明は、その他の信号を伝送する場合にも適用することが可能である。

【0065】

【発明の効果】以上の如く、請求項1に記載のデータ伝送装置および請求項4に記載のデータ伝送方法によれば、伝送するデータをスクランブルするためのキーを順次変更して所定のタイミングで発生し、発生されたキーを用いて伝送データをスクランブルし、データをスクランブルするのにそのとき用いられている第1のキーと、その次に用いられる第2のキーを伝送するようにしたので、デスクランブルの開始が、任意のタイミングにおいて実行可能な放送を実現することができる。

【0066】請求項5に記載のデータ受信装置および請求項7に記載のデータ受信方法によれば、伝送されてきたデータをスクランブルするのにそのとき用いられている第1のキーと、その次に用いられる第2のキーを抽出し、抽出されたキーから、第1のキーを選択し、選択した第1のキーを用いて、データをデスクランブルするようにしたので、スクランブルキーが適宜更新される場合においても、任意のタイミングからスクランブルされているデータをデスクランブルすることが可能となる。

【図面の簡単な説明】

【図1】本発明が適用される放送システムの構成例を示すブロック図である。

【図2】図1の受信端末2のより詳細な構成例を示すブ

11

ロック図である。

【図3】トランスポートパケットのフォーマットを説明する図である。

【図4】図1の実施例の動作を説明するタイミングチャートである。

【図5】transport_scrambling_controlを説明する図である。

【図6】従来のデータ伝送装置の動作を説明する図である。

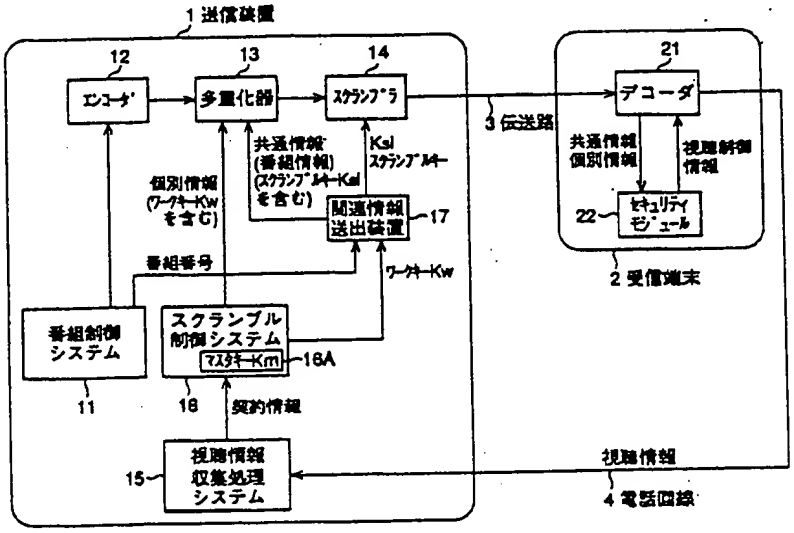
【符号の説明】

1　送信装置
2　受信端末
3　伝送路
4　電話回線
12　エンコーダ

12

13　多重化器
14　スクランブラ
16　スクランブル制御システム
16A　メモリ
17　関連情報送出装置
21　デコーダ
22　セキュリティモジュール
31　分離回路
32　デスクランブラ
33　選択回路
41　メモリ
42，43　復号器
44　メモリ
45　フラグ検出回路
47　分離回路

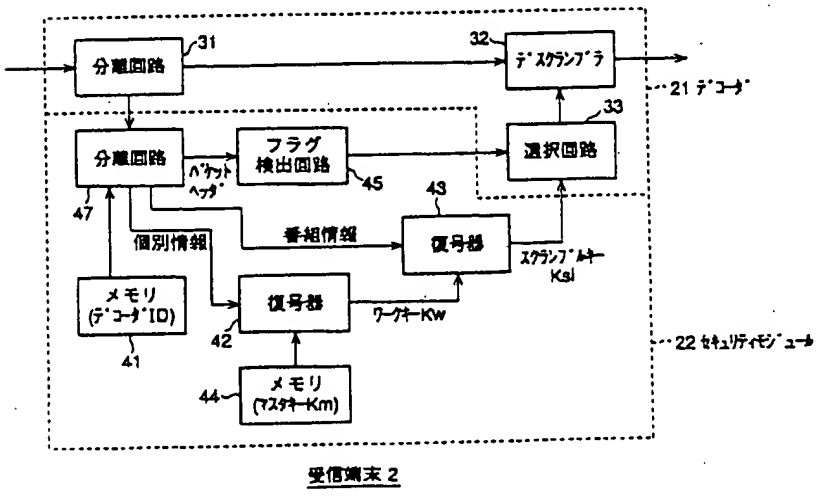
【図1】



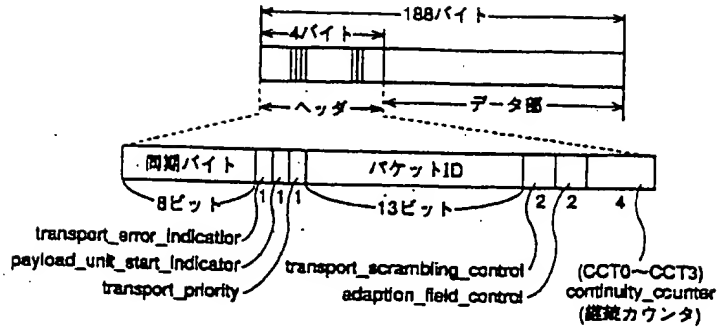
【図5】

transport_scrambling_controlフラグ例
10：スクランブルキーA系統使用
11：スクランブルキーB系統使用

【図2】

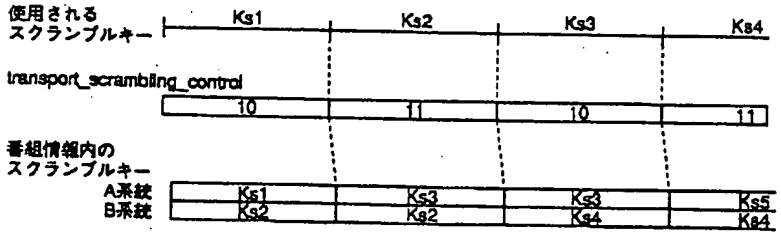


【図3】



トランスポートパケット

【図4】



【図6】